Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

Załącznik III do siwz

CZĘŚĆ III ZAMÓWIENIA

Dostawa routera – modularnego; przełącznika sieciowego umożliwiającego wirtualizację – **SZTUK 1 (jeden) - CPV 32413100-2 (rutery sieciowe)**

1. Architektura i wydajność urządzenia

- Urządzenie powinny być wyposażone w co najmniej dwa redundantne zasilacze zasilane z zewnątrz napięciem przemiennym 230V. Awaria jednego z zainstalowanych zasilaczy musi umożliwiać poprawną pracę urządzenia w pełnej konfiguracji.
- Router musi być wyposażony w matrycę przełączającą o architekturze “non-blocking”.
- Przepustowość matrycy powinna być dostępna dla wszystkich rozmiarów przełączanych pakietów z zakresu 64B-9180B.
- Przepustowość matrycy powinna mieć wielkość co najmniej 120 Gb full duplex.
- Urządzenie powinno umożliwiać przełączanie co najmniej 360 Mpps.
- Router powinien mieć możliwość zainstalowania redundantnej matrycy przełączającej. Wyłączenie lub awaria jednej z matryc, podczas gdy router jest wyposażony w redundantną matrycę przełączającą, nie może powodować przerwy w przełączaniu pakietów oraz nie może powodować degradacji wydajności urządzenia w czasie dłuższym niż 1 [s].
- Oferowane urządzenia powinny mieć architekturę modularną. Osobnymi modułami powinny być w szczególności:
  - zasilacze,
  - karty matryc przełączających i zarządzania/routingu,
  - karty interfejsów fizycznych,
  - moduły medium transmisyjnego (SFP lub XFP).
  - Urządzenia powinny umożliwiać rozbudowę (dodatkowe karty interfejsów) bez konieczności instalacji dodatkowej matrycy przełączającej przy zachowaniu wszystkich wymogów funkcjonalnych i wydajnościowych zawartych w niniejszej specyfikacji.
- Urządzenia powinny umożliwiać wymianę podzespołów redundantnych bez przerywania pracy urządzenia i degradacji wydajności na czas dłuższy niż 3 [s].
- Każdy z interfejsów powinien pracować z pełną prędkością w trybie pełnego dupleksu (ang. full duplex line-rate).
- Wymiana danych pomiędzy matrycą przełączającą a każdą z kart liniowych routera musi odbywać się z przepustowością umożliwiającą jednoczesną pracę każdego interfejsu na karcie liniowej z pełną prędkością medium (ang. line-rate) bez względu na pasmo zajmowane przez pojedynczy strumień danych. Powyższe wymagania muszą być spełnione dla przełączania ramek warstwy II modelu OSI oraz pakietów protokołów MPLS, IPv4 i IPv6.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

- Oferowane karty interfejsów muszą być w pełni wymienialne miedzy poszczególnymi urządzeniami.
- Wszystkie karty interfejsów 1GE oraz 10GE w ramach realizowanego zamówienia powinny mieć identyczną funkcjonalność.
- Karty interfejsów oraz moduły medium transmisyjnego powinny być wymienialne bez powodowania przerw w pracy całego urządzenia oraz bez konieczności wyłączania urządzenia.
- Wszystkie urządzenia powinny pracować pod kontrolą tego samego systemu operacyjnego i posiadać identyczny interfejs linii poleceń.
- Konfiguracja routera powinna być przechowywana w postaci tekstowego pliku konfiguracyjnego.
- Wymiary dostarczanych urządzeń powinny spełniać następujące wymagania:

szerokość [mm]	wysokość [mm]	głębokość [mm]
≤ 445	≤ 224	≤ 600

- Funkcjonalność routerów określonej kategorii, opisana w niniejszej specyfikacji musi być realizowana w obrębie jednego chassis. Nie dopuszcza się dostawy dodatkowych urządzeń rozszerzających funkcjonalność głównego routera (np.: media-konwertery, routery z interfejsami 100Base-FX/TX etc.).

2. Interfejsy fizyczne

- Router musi zawierać 2 interfejsy 10 GE i 20 interfejsów 1 GE
- Router powinien obsługiwać następujące moduły medium transmisyjnego zgodne z odpowiednimi standardami IEEE 802.3:
  - 10Base-T
  - 100Base-T
  - 100Base-FX (10km, 25km i 40km)
  - 1000Base-T
  - 1000Base-LX
  - 1000Base-SX
  - 10GBase-SR (300m)
  - 10GBase-LR (10km)
  - 10GBase-ER (40km)
  - 10GBase-ZR (80km)
- Wszystkie interfejsy fizyczne powinny umożliwiać wymianę modułu medium transmisyjnego w postaci standardowych, wymienialnych modułów SFP lub XFP.
- Elektryczne interfejsy Ethernet (Base-T) powinny pracować w trybie 10, 100 i 1000BaseT. Tryb pracy powinien być ustalany w procedurze auto-negocjacji lub przez konfigurację operatora.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

3. Funkcjonalność warstwy L2

- Dla wszystkich oferowanych interfejsów Ethernet, router powinien wspierać następujące funkcjonalności:
  - Bridging zgodnie z IEEE 802.1d,
  - VLAN Tagging zgodnie z IEEE 802.1p/Q,
  - VLAN stacking (Q-in-Q) zgodnie z IEEE 802.1ad,
  - Multiple Spanning Tree zgodnie z IEEE 802.1s,
  - Rapid Spanning Tree Protocol zgodnie z IEEE 802.1w,
  - Link Aggregation wraz protokołem LACP zgodnie z IEEE 802.3ad,
  - Ethernet OAM zgodnie z IEEE 802.3ah oraz zgodnie z IEEE 802.1ag.
  - IEEE 802.3x Flow Control.
- Router powinien obsługiwać (jednocześnie) pełen zakres (4094) identyfikatorów VLAN.
- Router powinien posiadać w pełni odseparowaną bazę adresów MAC (FIB) dla każdej instancji usługi L2. W szczególności powinna zachodzić możliwość duplikacji adresów MAC w poszczególnych instancjach usług L2.
- Router powinien obsługiwać identyfikatory VLAN o znaczeniu lokalnym dla portu fizycznego (ang. local vlan significance). Oznacza to m.in. iż ten sam identyfikator VLAN może być użyty na dowolnej liczbie pozostałych portów fizycznych.
- Router powinien wspierać translacje identyfikatorów VLAN, co oznacza iż usługa L2 może posiadać różne identyfikatory VLAN na poszczególnych portach.
- W ramach pojedynczej usługi L2 router powinien posiadać możliwość blokowania bezpośredniej komunikacji między portami w obrębie określonej grupy portów (ruch z portu należącego do danej grupy może zostać wysłany tylko do portów nienależących do tej grupy). Funkcjonalność ta powinna być niezależna od reguł filtrowania ACL.
- Dla wszystkich usług L2 powinna istnieć możliwość filtrowania ruchu w oparciu o następujące kryteria L2:
  - Źródłowy adres MAC,
  - Docelowy adres MAC,
  - EtherType,
- Dla wszystkich usług L2 powinna istnieć możliwość filtrowania ruchu w oparciu o następujące kryteria L3-L4:
  - Źródłowy adres IP wraz z maską,
  - Docelowy adres IP wraz z maską,
  - Typ protokołu,
  - Pakiet fragmentowany,
  - Źródłowy i docelowy port UDP wraz z maską,
  - Źródłowy i docelowy port TCP wraz z maską.
- Filtry powinny być przypisywane do interfejsów logicznych.
- Urządzenie powinno obsługiwać nie mniej niż 16 000 filtrów interfejsowych, oraz nie mniej niż 60 000 reguł filtrowania.
- Urządzenie powinno umożliwić zastosowanie co najmniej 16 000 reguł filtrowania do interfejsu bez wpływu na wydajność interfejsu, przy wielkości pakietów 64bajty. Wymaganie dotyczy interfejsów wszystkich typów (10Base-X, 100Base-X, 1GE, 10GE)

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

4. Funkcjonalność warstwy L2.5 / MPLS

- Router powinien wspierać MPLS oraz MPLS-TE zgodnie z RFC 2702, RFC 3031, RFC 3032 oraz RFC 3063.
- Router powinien wspierać (równocześnie) funkcjonalność LSR (Label Switch Router) jak i LER(Label Edge Router).
- Router powinien obsługiwać stos co najmniej 3 etykiet MPLS. Operacje PUSH i POP nie powinny mieć wpływu na wydajność pakietową.
- Funkcjonalność MPLS powinna być wspierana na wszystkich oferowanych interfejsach, w szczególności:
    - Interfejsach z enkapsulacją Ethernet 802.3/Eth-II,
    - Interfejsach z enkapsulacją IEEE 802.1Q,
    - Agregowanych interfejsach Ethernet (LAG).
- Router powinien implementować protokół LDP zgodnie z RFC 3036 oraz 3037, w szczególności powinien wspierać
    - Sesje Targeted LDP,
    - Autentykację sesji protokołem MD5,
    - Downstream Unsolicited Label Advertisment,
    - Ordered Control,
    - Liberal Label Retention Mode.
- Router powinien wspierać protokół RSVP-TE zgodnie z RFC 3209 oraz RFC 4090, w szczególności powinien wspierać :
    - Fast Re-Route w trybie one-to-one,
    - Fast Re-Route w trybie one-to-many (facility backup),
    - Protekcje LSP w trybie active – standby,
    - E-LSP.
- Router powinien wspierać LSP-ping oraz LSP-trace zgodnie z RFC 4379.
- Między daną parą węzłów może istnieć wiele ścieżek LSP, operator powinien mieć możliwość wskazania explicite z której ścieżki ma korzystać dana usługa.
- Router powinien umożliwiać zestawianie tuneli LDP wewnątrz tuneli RSVP (LDP-over-RSVP)

4.1. Usługi L2 VPN

4.1.1. Usługa Pseudo-Wire Emulation Edge-to-Edge (VLL)

- Router powinien wspierać usługę Ethernet L2 VPN punkt-punkt (Pseudo-Wire Emulation Edge-to-Edge) zgodnie z:
    - RFC 3985 PWE3,
    - RFC 4385 PWE3 Control Word for Use over an MPLS PSN,
    - RFC 3916 Requirements for PWE3,
    - RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

- Wsparcie usługi PWE3 powinno umożliwiać w pełni transparentne przenoszenie ramek Ethernet, w tym również ramek kontrolnych (BPDU). Ramki kontrolne nie mogą być przetwarzane przez moduły sterujące (ang. control plane).
- Zgodnie z RFC 4448 usługa Ethernet Pseudo-Wire powinna wspierać enkapsulację:
  - Typu Raw (tunelowana jest ramka 802.3/Eth-II)
  - Typu VLAN (tunelowana jest ramka 802.1Q)
- Porty dostępowe do usługi L2 VPN p2p powinna wspierać następującą enkapsulację:
  - Ethernet 802.3/Eth-II
  - Ethernet 802.1Q
  - Ethernet 802.1ad (Q-in-Q)
- Usługa L2 VPN p2p może być zestawiona między dowolną kombinacją wyżej wymienionych portów.
- Usługa L2 VPN p2p powinna umożliwiać następujące operacje na etykietach 802.1Q na interfejsie wejściowym:
  - Przyjęcie ramek Ethernet bez modyfikacji etykiet.
  - Zdjęcie pojedynczej etykiety 802.1Q
  - Zdjęcie dwóch etykiet 802.1Q
- Usługa L2 VPN p2p powinna umożliwiać następujące operacje na etykietach 802.1Q na interfejsie wyjściowym:
  - Przesłanie ramki bez modyfikacji etykiet.
  - Dodanie pojedynczej etykiety
  - Dodanie podwójnej etykiety
- Maksymalny rozmiar ramek L2 przenoszonych przez usługę L2 VPN p2p powinien być nie mniejszy niż 9100.
- Wartość MTU przenoszona przez usługę i negocjowana podczas zestawiania usług PWE3 powinna być explicite definiowana przez operatora.
- Router powinien wspierać co najmniej 4000 instancji usługi L2 VPN p2p, niezależnie od liczby pozostałych usług.
- Urządzenia powinny umożliwiać konfigurację czasu przechowywania adresów MAC (ang. aging) dla każdej instancji usługi L2VPN p2p.
- Usługa L2 VPN p2p powinna wspierać protekcje łącza PE-CE przez użycie protokołu LACP.
- Usługa L2 VPN p2p powinna wspierać protekcje węzła PE przez dołączenie urządzenia CE do dwóch węzłów PE (multi-homing).

4.1.2. Usługa Private Virtual LAN Service (VPLS)

- Router powinien wspierać usługę L2 VPN punkt-wielopunkt (VPLS) zgodnie z draft-ietf-l2vpn-vpls-ldp-01.
- Router powinien wspierać Hierarchical VPLS (H-VPLS).
- Wsparcie usługi PWE3 powinno umożliwiać w pełni transparentne przenoszenie ramek Ethernet, w tym również ramek kontrolnych (BPDU). Ramki kontrolne nie mogą być przetwarzane przez moduły sterujące (ang. control plane).
- Router powinien pozwalać na limitowanie ruchu użytkownika wchodzącego do danej instancji VPLS z podziałem na ruch typu:

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

  - Unicast,
  - Multicast,
  - Broadcast,
  - Unknown.

  Dla każdego typu ruchu powinna istnieć możliwość ustalenia innego limitu pasma i priorytetu.
- Porty dostępowe do usługi VPLS powinny wspierać następujące enkapsulacje:
  - Ethernet 802.3/Eth-II,
  - Ethernet 802.1Q,
  - Ethernet Q-in-Q.
- Usługa VPLS może być zestawiona między dowolną kombinacją wyżej wymienionych portów.
- Usługa VPLS powinna umożliwiać następujące operacje na etykietach 802.1Q, na interfejsie wejściowym:
  - Przyjęcie ramek Ethernet bez modyfikacji etykiet.
  - Zdjęcie pojedynczej etykiety 802.1Q
  - Zdjęcie dwóch etykiet 802.1Q
- Usługa VPLS powinna umożliwiać następujące operacje na etykietach 802.1Q na interfejsie wyjściowym:
  - Przesłanie ramki bez modyfikacji etykiet.
  - Dodanie pojedynczej etykiety
  - Dodanie podwójnej etykiety
- Maksymalny rozmiar ramek L2 przenoszonych przez usługę VPLS powinien być nie mniejszy niż 9180.
- Wartość MTU przenoszona przez usługę i negocjowana podczas zestawiania usług PWE3 powinna być explicite definiowana przez operatora.
- Router powinien wspierać co najmniej 4000 instancji usługi VPLS, niezależnie od liczby pozostałych usług.
- Pojemność tablicy MAC w skali całego routera powinna być nie mniejsza niż 120 tys. wpisów.
- Maksymalny rozmiar tablicy MAC per VPLS powinien być nie mniejszy niż 120 tys. wpisów.
- Powinna istnieć możliwość ograniczenia maksymalnej tablicy wpisów w tablicy MAC dla każdej instancji VPLS.
- Urządzenia powinny umożliwiać konfigurację czasu przechowywania adresów MAC (ang. aging) dla każdej instancji usługi VPLS.
- Powinna istnieć możliwość wyłączenia uczenia się adresów MAC w ramach określonej instancji VPLS.
- Router powinien wspierać mechanizm auto-discovery dla usługi VPLS.
- W usłudze VPLS powinna istnieć możliwość założenia filtrów „anty-spoofing”, bazujących na parze IP-MAC.
- Użycie filtrów „anty-spoofing” nie powinno wykluczać użycia innych filtrów ACL na tym samym porcie logicznym, w tej samej usłudze.
- Filtry anty-spoofing powinny być definiowane w systemie ręcznie lub automatycznie przez snooping DHCP.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

- Usługa VPLS powinna umożliwiać efektywną transmisje ruchu multicast, bez duplikacji pakietów multicastowych na tym samym łączu fizycznym, również w strukturach pierścieniowych.
- Usługa VPLS powinna wspierać transparentne przeniesieniu ruchu multicast bez interakcji z multicastowymi protokołami kontrolnymi.
- Usługa VPLS powinna wspierać funkcjonalność IGMP snooping, która pozwoli na duplikacje ruchu tylko na porty za którymi znajdują się odbiorcy.
    - IGMP-snooping powinien wspierać:
    - IGMPv1,
    - IGMPv2,
    - IGMPv3.
- Na portach dostępowych funkcja IGMP-snoopingu powinna być wspierana.
- W ramach usługi VPLS powinna istnieć możliwość uruchomienia protokołu spanning tree zgodnego z:
    - STP,
    - RSTP,
    - MSTP.
- Czas protekcji w usłudze VPLS, nie powinien przekraczać 50ms.

4.2. Usługi L3 VPN

- Router powinien wspierać usługi L3 VPN na wszystkich interfejsach liniowych zgodnie z:
    - draft-ietf-l3vpn-ospf-2547 OSPF as the PE/CE Protocol in BGP/MPLS IP VPNs,
    - RFC 4364 IP Virtual Private Networks (VPNs),
    - draft-ietf-l3vpn-2547bis-mcast-06 Multicast in MPLS/BGP IP VPNs,
    - draft-ietf-l3vpn-2547bis-mcast-bgp-04 BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs,
    - draft-ietf-l3vpn-e2e-rsvp-te-reqts-00 Requirements for supporting Customer RSVP and RSVP-TE over a BGP/MPLS IP-VPN,
    - RFC 3809 Generic Requirements for Provider Provisioned Virtual Private Networks,
    - RFC 4026 Provider Provisioned Virtual Private Network (VPN) Terminology,
    - RFC 4031 Service requirements for Layer 3 Provider Provisioned Virtual Private Networks,
    - RFC 4110 Framework for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs),
    - RFC 4111 Security Framework for Provider Provisioned Virtual Private Networks (PPVPNs),
    - RFC 4176 Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management,
    - RFC 4265 Definition of Textual Conventions for Virtual Private Network (VPN) Management,
    - RFC 4365 Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs),
    - RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs),
    - RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base,

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

- RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs),
- RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN,
- RFC 4684 Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protcol (IP) Virtual Private Networks (VPNs),
- RFC 4797 Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks.
- RFC 4834 Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private (PPVPNs).

5. Funkcjonalność warstwy L3

- Router powinien wspierać routing IP.
- Routing IP powinien być zaimplementowany sprzętowo.
- Router powinien rutować pakiety o rozmiarze 64 bajtów z szybkością interfejsu dla wszystkich obsługiwanych interfejsów, również przy pełnym obsadzeniu i obciążeniu wszystkich interfejsów.
- Router powinien obsługiwać co najmniej 10 milionów wpisów do głównej tablicy routingu (ang. Routing Information Base) dla protokołu Ipv4 oraz co najmniej 1,5 miliona wpisów do roboczej tablicy routingu na kartach liniowych (ang. Forwarding Information Base) dla protokołu Ipv4.
- Implementacja IP powinna być zgodna z:
  - RFC 791,
  - RFC 1812,
  - RFC 2460,
  - RFC 2461.
- Router powinien wspierać następujące protokoły:
  - ICMP zgodnie z RFC 792,
  - ARP zgodnie z RFC 826,
  - Proxy ARP zgodnie RFC 1027,
  - CIDR zgodnie z RFC 1519,
  - UDP zgodnie z RFC 768,
  - TCP zgodnie z RFC 791,
  - TFTP zgodnie z RFC 1350,
  - FTP zgodnie z RFC 959,
  - SSHv2,
  - BFD (Bidirectional Forwarding Detection) dla IPv4 zgodnie z draft-ietf-bfd-base-02 oraz draft-ietf-bfd-v4v6-1hop-02.txt,
  - VRRP (Virtual Router Redundancy Protocol) zgodnie z RFC 3768,
  - TACACS+ zgodnie z draft-grant-tacacs-02.txt,
  - RADIUS zgodnie z RFC 2865 oraz RFC 2865,
  - PPP zgodnie z RFC 1661,
  - PPP IPCP zgodnie z RFC 1332,
  - PPP OSILCP zgodnie z RFC 1377,

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

  - PPP BCP zgodnie z RFC 1638/2878,
  - PPP over SONET/SDH zgodnie z RFC 2615,
  - PPP Link Quality Monitoring zgodnie z RFC 1989 PPP,
  - DHCP zgodnie z RFC 2131,
  - DHCP Relay Agent Information Option (Option 82),
  - Interoperation between DHCP and BOOTP zgodnie z RFC 1534.
- Router powinien wspierać protokół BGP zgodnie z:
  - RFC 1771 BGPv4,
  - RFC 1745 BGP4/IDRP for IP-OSPF Interaction,
  - RFC 1997 BGP Communities Attribute,
  - RFC 2439 BGP Route Flap Damping,
  - RFC 2796 BGP Route Reflection,
  - RFC 1965 AS Confederations for BGP4 confederations,
  - RFC 2842 Capabilities Advertisement with BGP-4,
  - RFC 2918 Route Refresh Capability for BGP-4,
  - RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option.
- Router powinien umożliwiać współpracę z co najmniej 500 jednoczesnymi sąsiadami BGP.
- Router powinien wspierać protokół OSPF zgodnie z poniższymi standardami:
  - RFC 2328 OSPF Version 2
  - RFC 2370 Opaque LSA Support
  - RFC 3101 OSPF NSSA Option
  - RFC 3137 OSPF Stub Router Advertisement
  - RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
  - RFC 1765 OSPF Database Overflow
- Router powinien wspierać protokół ISIS zgodnie z poniższymi standardami:
  - RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO10589)
  - RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
  - RFC 2763 Dynamic Hostname Exchange for IS-IS
  - RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
  - RFC 2973 IS-IS Mesh Groups
  - RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
  - RFC 3567 Intermediate System to Intermediate System (ISIS) Cryptographic Authentication
- Router powinien wspierać protokół protokół RIP zgodnie z poniższymi standardami:
  - RFC 1058 RIP Version 1
  - RFC 2453 RIP Version 2
  - RFC 2082 RIP-2 MD5 Authentication
- Router powinien wspierać routing statyczny.
- Router powinien umożliwiać definiowanie preferencji dla informacji routingowych pochodzących z poszczególnych protokołów routingu.
- Router powinien umożliwiać definiowanie wielu (co najmniej 16) adresów IP dla każdego interfejsu logicznego (adres podstawowy i adresy dodatkowe).

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

- Router powinien wspierać redystrybucje informacji między poszczególnymi protokołami routingu.
- Redystrybucja powinna być realizowana przy pomocy reguł (polityk) importu i eksportu informacji.
- Router powinien wspierać Equal Cost Multi Path (ECMP) routing.
- Router powinien wspierać enkapsulację GRE (Generic Routing Encapsulation) zgodnie z RFC 1701, RFC 1702 oraz RFC 2784.
- Router powinien wspierać technologie point-to-multipoint wraz ze wsparciem link protection oraz node protection dla tej technologii.

6. Mechanizmy zarządzania jakością usługi

- Router powinien zapewniać dedykowane kolejki dla każdego interfejsu fizycznego.
- Router powinien wspierać co najmniej 8 dedykowanych kolejek dla każdego interfejsu fizycznego.
- Kolejki powinny być obsługiwane w trybie:
  - strict priority,
  - weighted round robin,
  - mieszanym.
- Klasyfikacja ruchu wejściowego powinna być możliwa na podstawie:
  - Pola 802.1p w ramkach Ethernet,
  - Pola EXP w pakietach MPLS,
  - Pola DSCP w pakietach IP,
  - Pola IP precedence w pakietach IP,
  - Filtrów L2 (kryteria: EtherType,src/dst MAC),
  - Fitrów L3-4 (kryteria: src/dst IP address, Protocol Type, src/dst port UDP/TCP).
- Router powinien umożliwiać modyfikacje następujących pól w pakietach wejściowych:
  - IEEE 802.1p,
  - IP Precedence,
  - DSCP,
  - MPLS EXP field.
  - Zmiana znakowania pakietów musi być możliwa w oparciu o trójkolorowy policer.
- Router powinien umożliwiać kontrolę pasma wejściowego poprzez policing.
- Router powinien umożliwiać kontrolę pasma wyjściowego przez:
  - Policing lub
  - Shaping,
- Kontrola pasma powinna być możliwa dla każdego portu z osobna.
- Implementacja QoS powinna być zgodna z DiffServ, określonym w:
  - RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
  - RFC 2597 Assured Forwarding PHB Group (rev3260)
  - RFC 2598 An Expedited Forwarding PHB
  - RFC 3140 Per-Hop Behavior Identification Codes
- Router powinien wspierać co najmniej 8 Forwarding Class (FC).
- Każda FC powinna mieć definiowalny priorytet oraz pasmo.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

7. Duplikacja ruchu

- Router powinien umożliwiać duplikacje ruchu i przesyłanie go do określonego portu wyjściowego (ang. mirroring).
- Router powinien umożliwiać duplikacje:
  - całego ruchu na porcie fizycznym,
  - ruchu z wybranego VLANu na porcie fizycznym.
- Router powinien umożliwiać zastosowanie filtrów ACL, które określały by jaki ruch będzie duplikowany.
- Router powinien umożliwiać wysłanie kopi ruchu:
  - do dowolnego innego portu na tym samym routeru,
  - do portu na innym routeru, używając do tego celu protokołu tunelowania.
- Powinna istnieć możliwość dodawania wybranego tagu 802.1q do kopii pakietów na porcie wyjściowym,
- Funkcja duplikacji nie powinna w żaden sposób zakłócać działania innych usług.
- Router powinien umożliwiać na uruchomienie co najmniej 250 instancji usługi duplikacji ruchu.

8. Mechanizmy bezpieczeństwa

- Powinna istnieć możliwość stopniowania praw dostępu do węzła dla poszczególnych użytkowników.
- Powinna istnieć możliwość uwierzytelniania i autoryzacji użytkowników w oparciu o:
  - Lokalną bazę użytkowników
  - Zewnętrzny serwer TACACS
  - Zewnętrzny serwer RADIUS
- Powinna istnieć możliwość autoryzacji każdej komendy wydawanej przez użytkowników w oparciu o:
  - Lokalną bazę użytkowników
  - Zewnętrzny serwer TACACS
  - Zewnętrzny serwer RADIUS
- Powinna istnieć możliwość rejestracji wszystkich komend wydawanych przez użytkownika za pomocą:
  - zapisywania ich w lokalnym pliku tekstowym
  - wysyłania ich do zewnętrznego serwera SYSLOG.
  - wysyłania ich zewnętrznego serwera TACACS
  - wysyłania ich zewnętrznego serwera RADIUS
- System powinien posiadać mechanizmy ochrony przed atakami DoS/DDoS. Między innymi powinna istnieć możliwość:
  - Zakładania list dostępowych (ACL) na ruch przeznaczony dla procesora urządzenia. Filtry te powinny być zakładane w jednym miejscu konfiguracji.
  - Limitowania poszczególnych typów ruchu przeznaczonego do procesora urządzenia.
  - Kolejność obsługi procesów przez procesor powinna uwzględniać ich priorytety.

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego
Inżynieria Internetu Przyszłości nr POIG 01.01.02-00-045/09-00

- Router powinien wspierać protokół NTPv4

Podsumowanie

Element	Ilość sztuk
Modularny przełącznik (router) sieciowy umożliwiający wirtualizację	1